GLENMERE COMMUNITY PRIMARY SCHOOL

At Glenmere we are GREAT! Because we:
Grow, Respect, Enjoy, Achieve Together

E-safety Policy and Procedure

Last updated: June 2023

Contents:

Statement of intent

Protecting young people and adults properly means thinking beyond the school environment. Broadband, Wi-Fi and 3/4G connections now mean the world wide web is available anywhere, anytime. Moreover, the introduction of the internet on games consoles, tablets and mobile phones mean it is becoming increasingly difficult to safeguard our children from the dangers hidden in cyberspace.

Our children will not only be working online in school or at home; their personal devices are not always covered by network protection and it is, therefore, imperative that they are educated on the risks involved with using the internet and are provided with guidance and a range of strategies on how to act if they see, hear or read something that makes them feel uncomfortable.

As a result, designing and implementing an E-safety Policy demands the involvement of a wide range of interest groups: the governors, headteacher, SLT, SENCO, DSL, classroom teachers, support staff, young people or parents, LA personnel, internet service providers (ISP), and regional broadband consortia, working closely with ISPs on network security measures.

E-safety is a child protection issue, and indeed it should not be managed primarily by the ICT team. It should be an extension of general safeguarding and led by the same people, so that, for instance, cyber bullying is considered alongside real-world bullying.

An E-safety Policy should:

- Allow young people to develop their own protection strategies for when adult supervision and technological protection are not available.
- Give information on where to seek help and how to report incidents.
- Help young people understand that they are not accountable for the actions that others may force upon them but that there are sanctions that the school will impose if they act inappropriately when online.
- Provide guidelines for parents and others on safe practice.
- Ensure you regularly monitor and review your policies with stakeholders.
- Ensure technological solutions are regularly reviewed and updated to ensure maintenance of an effective e-safety programme.

Above all, e-safety education should be a continuing feature of both staff development and young people's educational lifelong learning.

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at school with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of the school.
- Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.

Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.

Have clear structures to deal with online abuse, such as online bullying, which are cross referenced with other school policies.

Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

Minimise the risk of misplaced or malicious allegations made against adults who work with pupil.

Signed by:

	Headteacher	Date:	
	Chair of governors	Date:	

1. Teaching and learning

Why the internet and digital communications are important

1.1. The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience.

1.2. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

1.3. Teachers plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.

1.4. Staff model safe and responsible behaviour in their use of technology during lessons.

Internet use will enhance learning

1.5. The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

1.6. Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.

1.7. Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

1.8. Pupils will be shown how to publish and present information to a wider audience.

Pupils will be taught how to evaluate internet content

1.9. The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.

1.10. Pupils will be taught the importance of cross-checking information before accepting its accuracy.

1.11. Pupils will be taught how to report unpleasant internet content to their teacher. This can be done anonymously, or in person, and will be treated in confidence.

1.12. The school has a clear, progressive online safety education programme as part of the computing/PSHE curriculum. This covers a range of skills and behaviours appropriate to their age and experience, including:

To STOP and THINK before they CLICK.

To develop a range of strategies to evaluate and verify information before accepting its accuracy.

To be aware that the author of a website/page may have a bias or purpose and to develop skills to recognise what that may be.

To know how to narrow down or refine a search.

To understand how search engines work and to understand that this affects the results they see at the top of the listings.

To understand acceptable behaviour when using an online environment/email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private.

To understand how photographs can be manipulated and how web content can attract the wrong sort of attention.

To understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments.

To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos, and to know how to ensure they have turned-on privacy settings.

To understand why they must not post pictures or videos of others without their permission.

To know not to download any files – such as music files – without permission.

To have strategies for dealing with receipt of inappropriate materials.

To understand the impact of online bullying, sexting, extremism and trolling and know how to seek help if they are affected by any form of online bullying.

To know how to report any abuse, including online bullying, and how to seek help if they experience problems when using the internet and related technologies, i.e. parent, teacher or trusted staff member, or an organisation such as Childline or the CLICK CEOP button.

2. Managing internet access

Information system security

2.1. School ICT systems security will be reviewed regularly.

2.2. Virus protection will be updated regularly.

2.3. Security strategies will be discussed with the LA.

Email

2.4. Pupils may only use approved email accounts on the school system.

2.5. Pupils must immediately tell a teacher if they receive an offensive email.

2.6. In email communication, pupils must not reveal their personal details or those of others or arrange to meet anyone without specific permission.

2.7. Incoming emails will be treated as suspicious and attachments not opened unless the author is known.

2.8. The school will consider how emails from pupils to external bodies are presented and controlled.

2.9. The forwarding of chain letters is not permitted.

2.10. The school:

- Provides staff with an email account for their professional use (Microsoft 365)
- Does not publish personal email addresses of pupils or staff on the school website.
- Will contact the police if one of our staff or pupils receives an email that it considers is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up-to-date.
- Reports messages relating to or in support of illegal activities to the relevant authority and if necessary to the police.
- Knows that spam, phishing and virus attachments can make emails dangerous.

Published content and the school website

2.11. Staff or pupil personal contact information will not be published. The contact details given online should be the school office.

2.12. The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate, and the quality of presentation is maintained.

2.13. Uploading of information is restricted to our website authorisers.

2.14. The school website complies with the following statutory DfE guidelines for publications:

What academies, free schools and colleges should publish online

2.15. Most material is the school's own work; where others' work is published or linked to, we credit the sources used and state clearly the author's identity or status.

2.16. The point of contact on the website is the school address and telephone number. The school uses a general email contact address, office@glenmere.net. Home information or individual email identities will not be published.

2.17. Photographs published on the web do not have full names attached.

2.18. The school does not use pupils' names when saving images in the file names or in the tags when publishing to the school website.

Publishing pupils' images and work

2.19. Photographs that include pupils will be selected carefully and the school will consider using group photographs rather than full-face photos of individual children.

2.20. Pupils' full names will not be used anywhere on a school website or other online space, particularly in association with photographs.

2.21. Written permission from parents will be obtained before photographs of pupils are published on the school website.

2.22. Pupil image file names will not refer to the pupil by name.

2.23. Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

2.24. The school gains parental permission for use of digital photographs or video involving their child as part of the school agreement form when their child joins the school.

2.25. The school does not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs.

2.26. On trips and at events staff mainly use school devices, on occasions if they forget to take a school device, mobile phones can be used if the head teacher is informed. The images on return to school, must then be emailed to the ICT technician or school office and deleted immediately from the device.

2.27. If specific pupil photos (not group photos) are used on the school website, in the prospectus or in other high-profile publications, the school will obtain individual parental or pupil permission for their long-term use.

2.28. The school blocks/filters access to social networking sites or newsgroups unless there is a specific approved educational purpose.

2.29. Pupils are taught about how images can be manipulated in their e-safety education programme and to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work.

2.30. Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

2.31. Pupils are taught that they should not post images or videos of others without their permission. The school teaches them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. The school teaches them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Social networking and personal publishing

2.32. The school will control access to social networking sites and consider how to educate pupils in their safe use.

2.33. Newsgroups will be blocked unless a specific use is approved.

2.34. Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.

2.35. Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

2.36. Pupils will be advised to use nicknames and avatars when using social networking sites.

2.37. Staff will be reminded of the risks of accepting parents and children as 'friends' on social networking sites, will be strongly advised not to do so, and given advice on how to 'block' children from viewing their private pages.

2.38. Staff will be shown how to 'block' their profile picture from being downloaded and protect their profile information.

2.39. Staff will be encouraged to 'untag' themselves from any inappropriate pictures that may appear on social networking sites.

2.40. Teachers are instructed not to run social network spaces for pupil use on a personal basis or to open their own spaces to their pupils, but to use the school's preferred system for such communications.

2.41. School staff will ensure that in private use:

No reference should be made in social media to pupils, parents or school staff.

They do not engage in online discussion on personal matters relating to members of the school community.

Personal opinions should not be attributed to the school or LA.

Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Managing filtering

2.42. If staff or pupils come across unsuitable online materials, the site must be reported to the headteacher and ICT technician.

2.43. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Please see updated appendices g filtering and monitoring

Managing videoconferencing and webcam use

2.44. Videoconferencing should use the educational broadband network to ensure quality of service and security.

2.45. Pupils must ask permission from the supervising teacher before making or answering a videoconference call.

2.46. Videoconferencing and webcam use will be appropriately supervised.

Managing emerging technologies

2.47. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

2.48. The SLT should note that technologies, such as mobile phones with wireless internet access, can bypass school filtering systems and present a new route to undesirable material and communications.

2.49. Mobile phones will not be used by pupils during school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.

2.50. Staff may have their mobile phones with them during the day to answer work emails and to enable them to use them

2.51. The use by pupils of cameras in mobile phones will be kept under review.

2.52. Staff will not use personal mobile phones to communicate with children or use them to capture images of them.

Protecting personal data

2.53. Personal data will be recorded, processed, transferred and made available according to the GDPR and the Data Protection Act 2018.

Personal devices and mobile phones

2.54. The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided, except where it has been explicitly agreed otherwise by the headteacher. Images that are taken on personal devices must be emailed to the ICT technician and deleted immediately from the device.

2.55. The school reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand-held devices may be searched at any time as part of routine monitoring.

2.56. Where parents or pupils need to contact each other during the school day, they should do so only through the school's telephone. Staff may use their phones during break times. If a staff member is expecting a personal call, they must inform the headteacher and then take the call away from the children. Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from

2.57. Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.

2.58. Mobile phones and personally-owned devices can be used in the staff room and in the teacher's office during break and dinner for personal use.

2.59. The Bluetooth, or similar function, of a mobile phone will be switched off at all times and not be used to send images or files to other mobile phones.

2.60. Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.

2.61. Staff will use the school phone to make contact with parents.

2.62. Mobile phones will be used to message staff if the school is

2.63. If a member of staff breaches the school policy, disciplinary action may be taken.

2.64. In an emergency where a staff member doesn't have access to a school-owned device on an out of activity event, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes. Where possible the member of staff should ring the school office for the office to make contact with the parents.

2.65. Pupils will abide by the following rules when using personal devices in school:

The school strongly advises that pupil mobile phones should not be brought into school; however, we accept that there may be circumstances in which a parent wishes their child to have a mobile phone for their own safety.
Only y6 children are allowed to bring mobile phones into school and these are handed in to the class teacher at the start of the day and returned at the end of the day.

3. Policy decisions

Authorising internet access

3.1. All staff will read and sign the Staff, Governor and Visitor Acceptable Use Agreement before using any school ICT resource.

3.2. The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

3.3. At EYFS and KS1, access to the internet will be by adult demonstration with directly supervised access to specific, approved online materials.

3.4. Any person not directly employed by the school will be asked to sign the Staff, Governor and Visitor Acceptable Use Agreement before being allowed to access the internet from the school site.

Assessing risks

3.5. The school will take all reasonable precautions to prevent access to inappropriate material; however, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor the LA can accept liability for any material accessed, or any consequences of internet access.

3.6. The school should audit ICT use to establish if the E-safety Policy is adequate and that the implementation of the E-safety Policy is appropriate and effective.

Handling e-safety complaints

3.7. Complaints of internet misuse will be dealt with by a senior member of staff.

3.8. Any complaint about staff misuse must be referred to the headteacher.

3.9. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

3.10. Pupils and parents will be informed of the complaints procedure (see school's complaints policy)

3.11. Pupils and parents will be informed of the consequences for pupils misusing the internet.

3.12. Discussions will be held with the police to establish procedures for handling potentially illegal issues.

Community use of the internet

3.13. The school will liaise with local organisations to establish a common approach to e-safety, if necessary.

4. Pupil online safety curriculum

Teaching and learning

4.1. This school has a clear, progressive online safety education programme as part of the computing/PSHE curriculum. This covers a range of skills and behaviours appropriate to the age of the children, including:

To STOP and THINK before they CLICK.

To develop a range of strategies to evaluate and verify information before accepting its accuracy.

To know how to narrow down or refine a search.

To understand acceptable behaviour when using an online environment/email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private.

To understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments.

To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings.

To have strategies for dealing with receipt of inappropriate materials.

To understand the impact of online bullying, sexting, extremism and trolling and know how to seek help if they are affected by any form of online bullying.

To know how to report any abuse, including online bullying, and how to seek help if they experience problems when using the internet and related technologies, i.e. parent, teacher or trusted staff member, or an organisation such as Childline.

4.2. Teachers plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.

4.3. All staff will model safe and responsible behaviour in their own use of technology during lessons.

Online risks

4.4. The school recognises that pupils increasingly use a range of technology such as mobile phones, tablets, games consoles and computers. It will support and enable children to use these technologies for entertainment and education but will also teach children (in PSHE) that some adults and young people will use such outlets to harm children.

Cyber bullying and abuse

4.5. Cyber bullying can be defined as “Any form of bullying which takes place online or through smartphones and tablets.” - BullyingUK

4.6. Complaints of online bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school/LA child protection procedures.

4.7. Through the PSHE curriculum, children are taught to tell a responsible adult if they receive inappropriate, abusive or harmful emails or text messages..

4.8. Cyber bullying will be treated as seriously as any other form of bullying and will be managed through our anti-bullying and confiscation procedures. Cyber bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school’s policy on anti-bullying and behaviour.

4.9. There are clear procedures in place to support anyone in the school community affected by cyber bullying.

4.10. All incidents of cyber bullying reported to the school will be recorded.

Sexual exploitation/sexting

4.11. Sexting between pupils will be managed through our anti-bullying and confiscation procedures.

4.12. All staff are made aware of the indicators of sexual exploitation and all concerns are reported immediately to the DSL.

4.13. There are clear procedures in place to support anyone in the school community affected by sexting.

4.14. All incidents of sexting reported to the school will be recorded.

Radicalisation or extremism

4.15. Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism leading to terrorism.

4.16. Extremism is defined by the Crown Prosecution Service as “The demonstration of unacceptable behaviour by using any means or medium to express views which:

Encourage, justify or glorify terrorist violence in furtherance of beliefs.
Seek to provoke others to terrorist acts.
Encourage other serious criminal activity or seek to provoke others to serious criminal acts.
Foster hatred which might lead to inter-community violence in the UK.”

4.17. The school understands that here is no such thing as a “typical extremist”: those who become involved in extremist actions come from a range of backgrounds and experiences, and most individuals, even those who hold radical views, do not become involved in violent extremist activity.

4.18. The school understands that pupils may become susceptible to radicalisation through a range of social, personal and environmental factors – it is known that violent extremists exploit vulnerabilities in individuals to drive a wedge between them and their families and communities. It is vital that school staff can recognise those vulnerabilities.

4.19. Staff will maintain and apply a good understanding of the relevant guidance to prevent pupils from becoming involved in terrorism.

4.20. The school will monitor its RE curriculum and assembly policy to ensure that they are used to promote community cohesion and tolerance of different faiths and beliefs.

4.21. Senior leaders will raise awareness within the school about the safeguarding processes relating to protecting pupils from radicalisation and involvement in terrorism.

5. Communications policy

Introducing the E-safety Policy to pupils

5.1. E-safety rules and guidance will be delivered on a regular basis to the pupils.

5.2. Pupils will be informed that network and internet use will be monitored and appropriately followed up.

5.3. A programme of training in e-safety will be developed by the ICT technician, ICT co-ordinator,PSHE co-ordinator and in conjunction with all teachers.

5.4. Safety training will be embedded within the computing and PSHE schemes of work in line with national curriculum expectations.

Staff and the e-safety policy

5.5. All staff will be given the school E-safety Policy and have its importance explained.

5.6. Staff must be informed that network and internet traffic can be monitored and traced to the individual user.

5.7. Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.

5.8. Staff will always use a child friendly safe search engine when accessing the web with pupils.

Enlisting parents' support

Parents' attention will be drawn to the school E-safety Policy in an e-safety leaflet, newsletters, the school brochure and on the school website.

The school will maintain a list of e-safety resources for parents.

The school will ask all new parents to sign the parent/pupil agreement when they register their child with the school.

The school will have a page on its website dedicated to keeping children safe online. It will provide parents with useful links to help them in understanding the internet.

E-safety Activities and Issues

Activities	Key e-safety issues
Creating web directories to provide easy access to suitable websites	Parental consent should be sought Pupils should be supervised Pupils should be directed to specific, approved online materials
Using search engines to access information from a range of websites	Filtering must be active and checked frequently Parental consent should be sought Pupils should be supervised Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with
Exchanging information with other pupils and asking questions of experts via email or blogs	Pupils should only use approved email accounts or blogs Pupils should never give out personal information
Publishing pupils' work on school and other websites	Pupil and parental consent should be sought prior to publication Pupils' full names and other personal information should be omitted Pupils' work should only be published on moderated sites and only by the ICT technician.
Publishing images, including photographs of pupils	Parental consent for publication of photographs should be sought through GDPR agreement File names should not refer to the pupil by name Staff must ensure that published images do not breach copyright laws
Communicating ideas within chat rooms or online forums	Only chat rooms dedicated to educational use and that are moderated should be used Access to other social networking sites should be blocked Pupils should never give out personal information
Audio and video conferencing to gather information and share pupils' work	Pupils should be supervised The school should only use applications that are managed by LAs and approved educational suppliers
Social networking	Staff should set their profiles to private and ensure they do not accept friend requests from pupils or parents Social networking sites should be blocked on the school network Pupils should be educated in the dangers involved in 'friending' or talking to people they do not know online

Useful Resources for Teachers and Parents

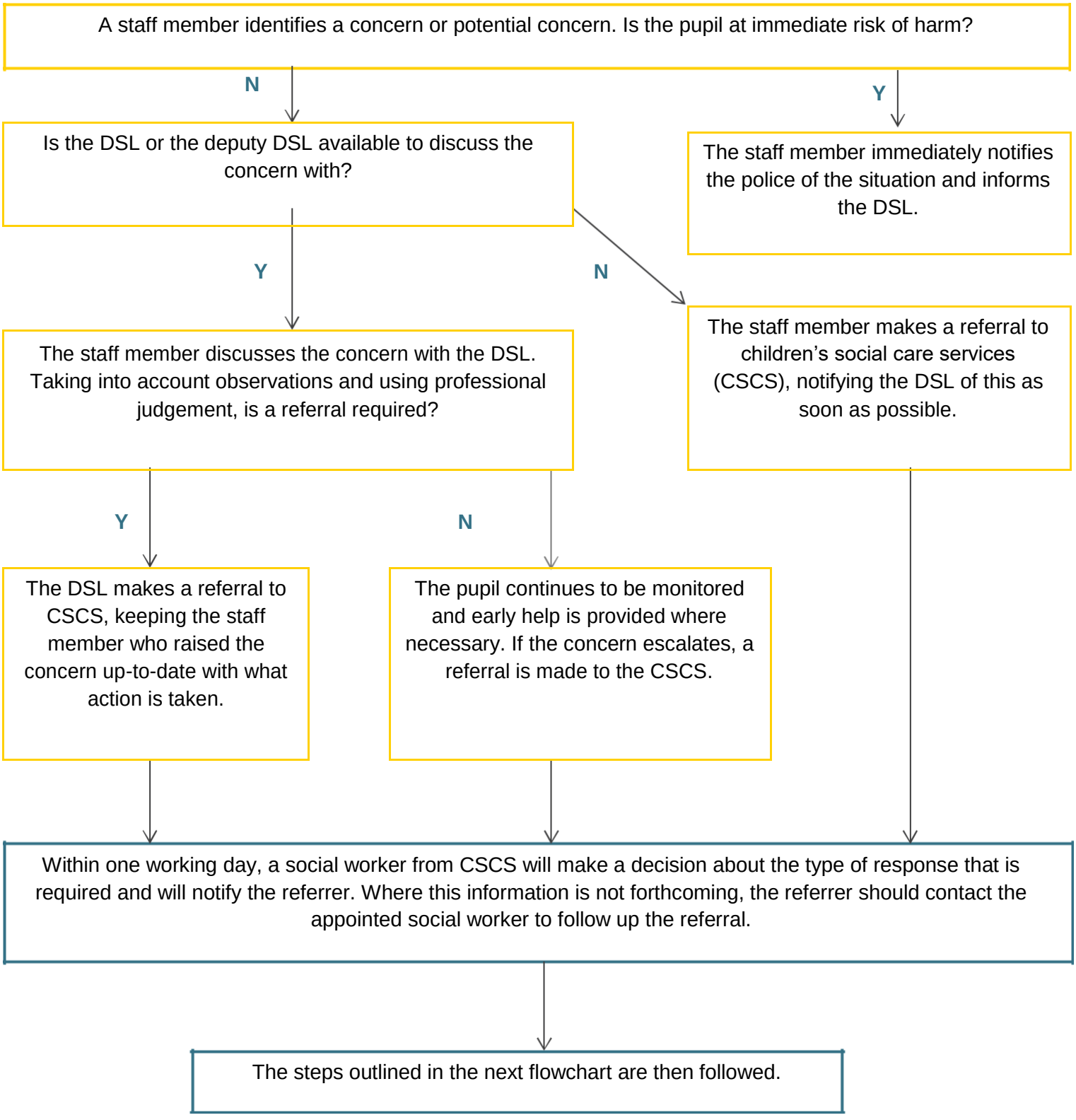
Resource	Website
Child Exploitation and Online Protection Centre	www.ceop.gov.uk/
Childnet	www.childnet-int.org/
Digizen	www.digizen.org/
Kidsmart	www.kidsmart.org.uk/
Think U Know	www.thinkuknow.co.uk/
Family Online Safety Institute	http://www.fosi.org
Internet Watch Foundation	www.iwf.org.uk
Internet Safety Zone	www.internetsafetyzone.com
Vodafone digital parenting	www.vodafone.com/content/digital-parenting.html
NSPCC - Share Aware	www.nspcc.org.uk/preventing-abuse/keeping-children-safe/share-aware
Parent Zone	www.theparentzone.co.uk/school

Response to an Incident of Concern Flowchart

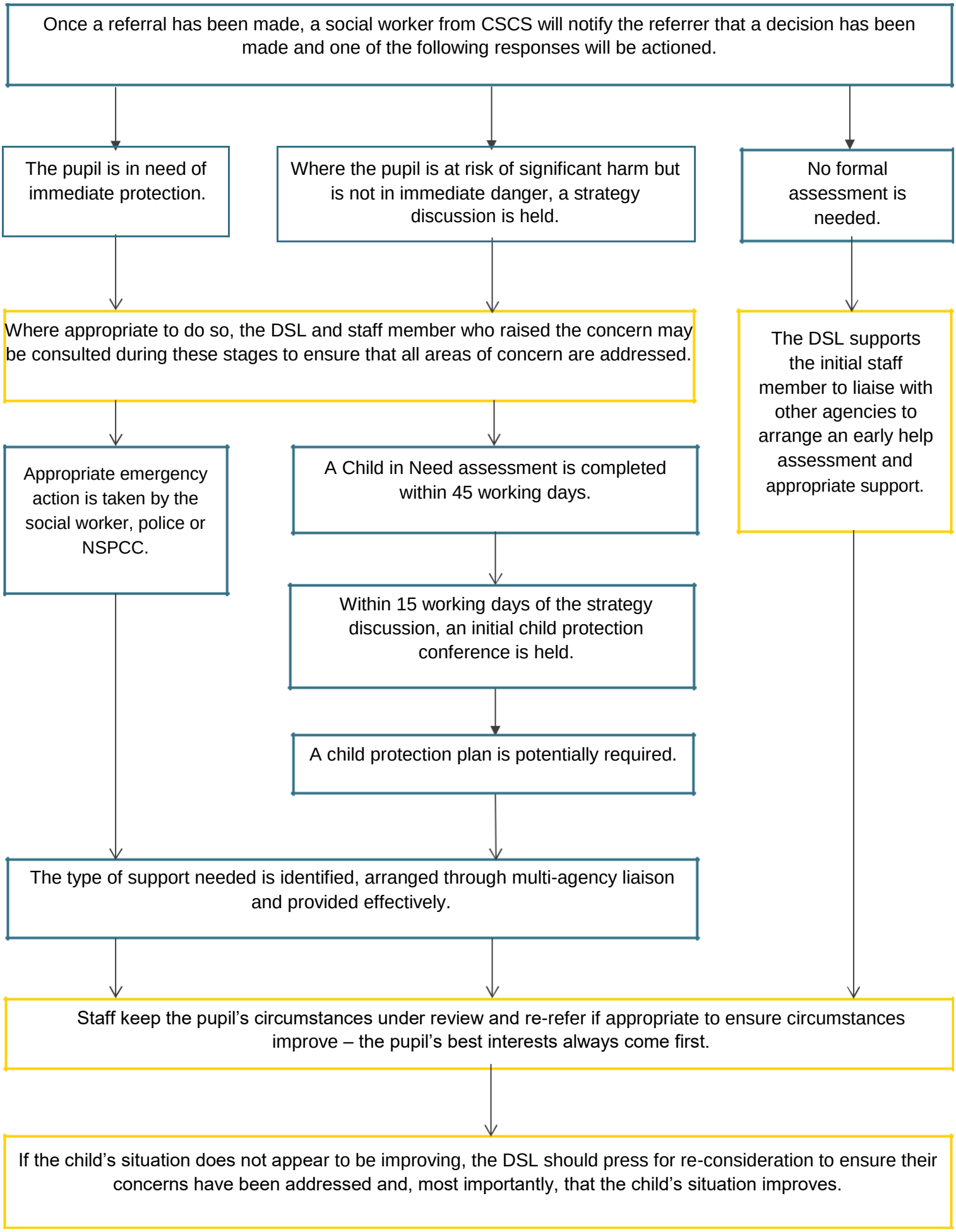
The process outlined within the first section should be followed where a staff member has a safeguarding concern about a child. Where a referral has been made, the process outlined in the 'After a referral is made' section should be followed.

The actions taken by the school are outlined in yellow, whereas actions taken by another agency are outlined in blue.

Before a referral is made



After a referral is made



Staff, Governor and Visitor Acceptable Use Agreement

ICT and the related technologies, such as email, the internet and mobile devices, are an expected part of daily working life in school. This policy is to help ensure that all staff are aware of their professional responsibilities when using any form of ICT and to help keep staff, governors and visitors safe. All staff are expected to sign this agreement confirming their undertaking to adhere to its contents at all times. Any concerns or clarification should be discussed with the headteacher.

I will only use the school's email, internet, learning platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the **headteacher** or **governing board**.

I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.

I will ensure that all electronic communications with pupils and staff are compatible with my professional role.

I will not give out my personal details, such as mobile phone number or personal email address, to pupils.

I will only use the approved email system for any communications with pupils, parents and other school-related activities.

I will ensure that personal data (such as data held on the administration system) is kept secure and is used appropriately. Personal data can only be taken out of the school or accessed remotely when authorised by the headteacher or governing body and with appropriate levels of security in place.

I will not install any hardware or software on school equipment without the permission of the headteacher/ICT technician.

I will report any accidental access to inappropriate materials immediately to the headteacher.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with data protection policy and with written consent of the parent or staff member. Images will not be distributed outside the school network without the permission of the parent, member of staff or headteacher in line with data security policy.

I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to the headteacher.

I will respect copyright and intellectual property rights.

I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute. This includes ignoring invitations from pupils and parents to be part of their social networking site(s).

I will support and promote the school's E-safety Policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User signature

I agree to follow this acceptable use policy and to support the safe use of ICT throughout the school.

Signature _____

Date _____

Full name _____ (Printed)

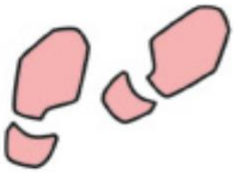
[Primary schools only] Rules for EYFS and KS1

Think then Click

These rules help us to stay safe on the

internet E-safety rules for EYFS and KS1

- ✓ We only use the internet when an adult is with us.
- ✓ We can click on the buttons or links when we know what they do or where they take us.
- ✓ We can use the internet to search for things when an adult is with us.
- ✓ We always stop and ask for help if we get lost on the internet.
- ✓ We can send and open emails with a grown-up.
- ✓ We can write polite and friendly emails to people we know.
- ✓ We never share our names or addresses on the internet.
- ✓ We know that friends are people we know in the real world not people we meet online.



[Primary schools only] Rules for KS2

Think then Click

These rules help us to stay safe on the internet

E-safety rules for KS2

- ✓ We ask permission before using the internet.
- ✓ We only look at websites an adult has given us permission to use.
- ✓ We always tell an adult if we have seen, heard or read anything on the internet that has made us feel threatened, uncomfortable or worried.
- ✓ We immediately close a web page if we are unsure.
- ✓ We only send polite and friendly emails to people we know or that an adult has approved.
- ✓ We never give out personal information or passwords.
- ✓ We never arrange to meet anyone we don't know.
- ✓ We do not open emails sent by anyone we don't know.
- ✓ We do not use internet chat rooms.
- ✓ We know that friends are people we know in the real world not people we meet online.




Appendix G - School Filtering and Monitoring

Introduction

The filtering of internet content provides an important means of preventing users from accessing material thatis illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Glenmere Community Primary School IT service is Netsweeper supplied by and managed by ekte.
The following information from UKSafer Internet Centre references how this is provided.

Ekte Solutions look after the web filtering for school and will ensure that:

- The service is maintained and accessible for schools to use
- All relevant safeguards are being met
- School is taking necessary precautions to ensure the service provided is

appropriateEkte will also investigate any web filtering related issues including:

- Access to websites containing inappropriate or potentially harmful material
- Access to websites containing educational or related material deemed appropriate for school
- Provide web access reports on an annual basis

Ekte works to ensure that the UK Safer Internet Centre checklist is followed. The web filtering service meets and exceeds the Ofsted guidelines. The solution is constantly updated via national feeds from the wider Internet community to ensure that as new websites are created they are categorised and sanctioned accordingly.

Above the web filtering aspect of the service, Ekte also provides the following features:

- Application Control – this stops some applications running which utilise peer to peer (file-sharing) features
- Intrusion Prevention – this is aimed at stopping hackers from gaining access to your endpoints
- Website Certificate Inspection – this checks websites to ensure any certificates are valid and up todate. This stops users accessing malicious websites or websites that are not properly maintained.

Schools (and registered childcare providers) in England and Wales are required “to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering” (Revised Prevent Duty Guidance: for England and Wales)
Furthermore, it expects that they “assess the risk of [their] children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology”.
Department for Education’s statutory guidance ‘Keeping Children Safe in Education’ obliges schools and colleges in England to “ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system” however, schools will need to “be careful that “over blocking” does not lead to unreasonable restrictions as towhat children can be taught with regards to online teaching and safeguarding.”

From the information provided to us by our supplier Ekte, we are confident that the web filtering solution as configured meets the current DfE guidance. Netsweeper filtering is a safe, secure and a tested system. The following data has alsobeen collected and tested by ‘UK Safer Internet Centre’. We have provided the following information to assist in reaffirming your confidence and understanding of the Netsweeper system.

Many of the questions and requirements have been addressed in the Netsweeper submission to the 'Safe Internet Centre', copied below, for the original please select the following link.

https://saferinternet.org.uk/resource/2021-netsweeper-monitoring-provider-response

Appropriate Monitoring for Schools

May 2023

Monitoring Provider Checklist Reponses

Schools (and registered childcare providers) in England and Wales are required "to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering". Furthermore, it expects that they "assess the risk of [their] children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology". There are a number of self review systems (eg www.360safe.org.uk) that will support a school in assessing their wider online safety policy and practice.

The Department for Education's statutory guidance 'Keeping Children Safe in Education' obliges schools and colleges in England to "*ensure appropriate filters and appropriate monitoring systems are in place and regularly review their effectiveness" and they "should be doing all that they reasonably can to limit children's exposure to [Content, Contact, Conduct, Contract] risks from the school's or college's IT system*" however, schools will need to "*be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding*."

By completing all fields and returning to UK Safer Internet Centre (enquiries@saferinternet.org.uk), the aim of this document is to help monitoring providers to illustrate to schools how their particular technology system(s) meets the national defined 'appropriate monitoring' standards. Fully completed forms will be hosted on the UK Safer Internet Centre website alongside the definitions

The results will help schools better assess, in conjunction with their completed risk assessment, if the monitoring system is 'appropriate' for them.

Company / Organisation	Netsweeper
Address	Suite 125-126 Pure Offices, 4100 Park Approach Thorpe Park, Leeds United Kingdom LS15 8GB
Contact details	Nick levey
Monitoring System	Onguard
Date of assessment	10/06/2023

System Rating response

Where a supplier is able to confirm that their service fully meets the issue identified in a specific checklist the appropriate self-certification colour forthat question is GREEN.	
Where a supplier is not able to confirm that their service fully meets the issue identified in a specific checklist question the appropriate self-certification colour for that question is AMBER.	

Monitoring Content

Monitoring providers should ensure that they:

Aspect	Rating	Explanation
• Are IWF members		We are IWF member
• Utilisation of IWF URL list for the attempted access of known child abuse images		We integrate this list into our products along with several others
• Work with CTIRU 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		We integrate this list
• Confirm that monitoring for illegal content cannot be disabled by the school		This can be deployed so thatit is unremovable

Inappropriate Online Content

Monitoring providers should both confirm, and describe how, their system monitors/manages the following content

Content	Explanatory notes – Content that:	Rating	Explanation
Illegal	content that is illegal, for example child abuse images and unlawful terrorist content		Netsweeper uses dynamic content analysis to categories , this and many other content types.
Bullying	Involve the repeated use of force, threat or coercion to abuse, intimidate or aggressively dominate others		Netsweeper uses dynamic content analysis to categories , this and many other content types.
Child Sexual Exploitation	Is encouraging the child into a coercive/manipulative sexual relationship. This may include encouragement to meet		Netsweeper uses dynamic content analysis to categories , this and many other content types.
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, sex, disability or gender identity		Netsweeper uses dynamic content analysis to categories , this and many other content types.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		Netsweeper uses dynamic content analysis to categories , this and many other content types.

Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		Netsweeper uses dynamic content analysis to categories , this and many other content types.
Gambling	Enables gambling		Netsweeper uses dynamic content analysis to categories , this and many other content types.
Pornography	displays sexual acts or explicit images		Netsweeper uses dynamic content analysis to categories , this and many other content types.
Self Harm	promotes or displays deliberate self harm		Netsweeper uses dynamic content analysis to categories , this and many other content types.
Suicide	Suggest the user is considering suicide		Netsweeper uses dynamic content analysis to categories , this and many other content types.
Violence	Displays or promotes the use of physical force intended to hurt or kill		Netsweeper uses dynamic content analysis to categories , this and many other content types.

Monitoring System Features

How does the monitoring system meet the following principles:

Principle	Rating	Explanation
• Age appropriate – includes the ability to implement variable monitoring appropriate toage and vulnerability. This will in turn define which alerts are prioritised and responded to.Further situations may warrant additional capability, for examples boarding schools or community based access		Monitoring is broken down into various categories and and priority levels to allow the school to take a gradiated response based on age or vulnerability
• Alert Management – how alerts are managed – if schools manage system alerts or support/management is provided		A managed service is provided , however schools can still manage their own alerts of so desired
• Audit – Any changes to the monitoring system are logged enabling an audit trail that ensures transparency and that individuals are not able to make unilateral changes.		All changes as logged and auditable. As are all other aspects of usage
• BYOD (Bring Your Own Device) – if the system includes the capability to monitor personal mobile and app technologies (ie not owned by the school), how is this deployed and supportedand how data is managed. Does it monitor beyond the school hours and location		Schools can choose to monitor BYOD devices. How this is done is dependant on the schools policy and attitude to risk

• Data retention –what data is stored, where is it (physically– ie cloud/school infrastructure) stored and for how long. This should also include any data backup provision		All data is stored in the UK. Data retention is definable by the customer.
• Devices – if software is required to be installed on devices, the monitoring system should be clear about the devices (and operating systems)it covers		Safeguarding functionality is available for windows, mac, chromebook, ios and android.
• Flexibility - changes in keywords (addition or subtraction) can be easily amended accordingto an agreed policy		Keyword lists can be amended for web based content
• Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		The system is multitenant and allows for this level of control
• Monitoring Policy – How are all users madeaware that their online access is being monitored? Is any advice or guidance provided to support schools?		Guidance can br provided but each school must make their own decisions
• Multiple language support – the ability for the system to manage relevant languages?		Multiple languages are supported
• Prioritisation – How are alerts generated and prioritised to enable a rapid response to immediate issues. What operational procedures are in place to facilitate that process?		All alerts are broken down into both subject and prioritisation categories, instant alerting varies based on the severity of the incident
• Remote monitoring – with many children and staff working remotely, the ability, extent and management for the monitoring of devices (school and/or personal). Included here is the hours of operation together with the explicit awareness of users.		Netsweeper offers remote monitoring on various SLA's
• Reporting – how alerts are recorded within the system?		Alerts are recorded within the system itself and logged , they can then be exported if required
• Harmful Image detection – The inclusion or extent to which visual content is discovered, monitored and analysed (eg Image hash)		Done using specialist lists provided by various agencies. This includes IWF and CAIC

Pro Active Monitoring - how any pro-active monitoring support is provided including if any automation is utilised and the safeguarding capability of the organisation's teams.

Netsweeper provides pro active monitoring support with an inhouse team of UK based monitoring experts. Our team members are specifically selected for safeguarding skillsets and go through specific training form recognised external providers.

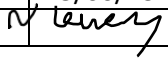
Please note below opportunities or enhancements to support schools (and other settings) with their obligationsaround Keeping Children Safe in Education?

Netsweeper provides filtering , safeguarding and monitoring products together with training packages around safeguarding and technology

MONITORING PROVIDER SELF-CERTIFICATION DECLARATION

In order that schools can be confident regarding the accuracy of the self-certification statements, the supplierconfirms:

- that their self-certification responses have been fully and accurately completed by a person or persons whoare competent in the relevant fields
- that they will update their self-certification responses promptly when changes to the service or its terms andconditions would result in their existing compliance statement no longer being accurate or complete
- that they will provide any additional information or clarification sought as part of the selfcertificationprocess
- that if at any time, the UK Safer Internet Centre is of the view that any element or elements of a provider's self-certification responses require independent verification, they will agree to that independent verification,supply all necessary clarification requested, meet the associated verification costs, or withdraw their self- certification submission.

Name	Nick Levey
Position	Regional Director
Date	15/06/23
Signature	

Responsibilities

The responsibility for the management of the school's filtering and monitoring policy will be held by the DSL, Computing Lead, Technician, supported by ekte netsweeper. They will manage the school filtering, in line with this policy and will keep records/logs of changes and of breaches of the filtering systems.

All users have a responsibility to report immediately to the DSL any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programs or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials.

Education/Training/Awareness

Pupils will be made aware of the importance of filtering systems through the E-Safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- signing the AUP
- induction training
- staff meetings, briefings, Inset

Parents will be informed of the school's filtering policy through the Acceptable Use agreement.

Changes to the Filtering System

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the headteacher who will decide whether to make school level changes (as above). If it is felt that the site should be filtered (or unfiltered), the technician should contact Ekte with the URL.